(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－49493

(43)公開日　平成10年(1998)２月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｂ
	1/00	３７０			1/00	３７０Ｅ
	11/30	３２０			11/30	３２０Ｅ
	13/14	３３０			13/14	３３０Ｚ

審査請求　有　　請求項の数３　ＯＬ　（全５頁）

(21)出願番号　特願平8－206717

(22)出願日　平成８年(1996)８月６日

(71)出願人　000190541
新潟日本電気株式会社
新潟県柏崎市大字安田7546番地

(72)発明者　樋口　敏明
新潟県柏崎市大字安田7546番地新潟日本電気株式会社内

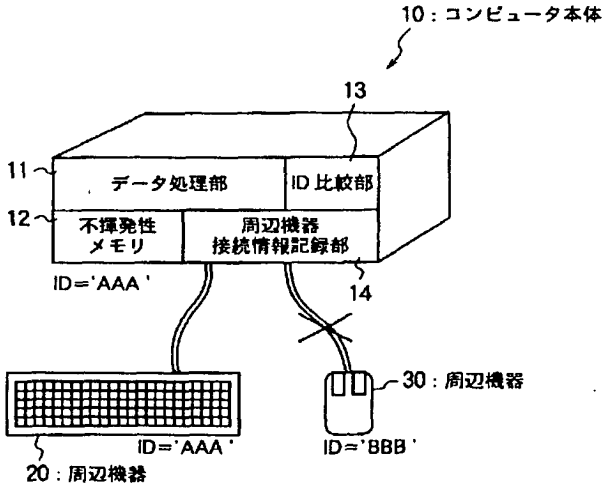
(74)代理人　弁理士　稲垣　清

(54)【発明の名称】　コンピュータシステム

(57)【要約】

【課題】　コンピュータシステムの周辺機器の盗難を防ぐ。

【解決手段】　コンピュータ本体１０及び周辺機器２０、３０に夫々識別番号を登録する不揮発性メモリを設け、コンピュータ本体２０には、更に、コンピュータ本体の不揮発性メモリ１２に登録された識別番号と周辺機器２０、３０の不揮発性メモリに登録された識別番号とを比較する識別番号比較部１３と、識別番号比較部１３の比較結果に基づいて周辺機器の使用を許可又は不許可とする周辺機器使用判定部１４とを設ける。周辺機器は、登録された特定のコンピュータシステム以外では使用できなく、盗品の周辺機器の経済的価値は殆どなくなるので、周辺機器の盗難が抑止される。



1

【特許請求の範囲】

【請求項１】　コンピュータ本体と、該コンピュータ本体に接続される少なくとも１つの周辺機器とを備えるコンピュータシステムにおいて、

コンピュータ本体及び周辺機器に夫々識別番号を登録する不揮発性メモリを設け、

前記コンピュータ本体が、該コンピュータ本体の不揮発性メモリに登録された識別番号と周辺機器の不揮発性メモリに登録された識別番号とを比較する識別番号比較部と、該識別番号比較部の比較結果に基づいて周辺機器の使用を許可又は不許可とする周辺機器使用判定部とを備えることを特徴とするコンピュータシステム。

【請求項２】　前記周辺機器使用判定部は、前記周辺機器の不揮発性メモリに識別番号を登録する機能を更に有する、請求項１に記載のコンピュータシステム。

【請求項３】　前記識別番号比較部は、オペレータによって入力された識別番号と、前記コンピュータ本体の不揮発性メモリに登録された識別番号とを比較する機能を更に有する、請求項１又は２に記載のコンピュータシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータシステムに関し、特にコンピュータシステムの周辺機器の盗難を抑止するためのセキュリティ技術に関する。

【０００２】

【従来の技術】コンピュータシステムのセキュリティとしては、コンピュータシステムに記録されたデータの保護と、コンピュータシステムを構成する装置の盗難防止の２つが重要である。コンピュータシステムにおけるデータのセキュリティに関しては、従来、内部データの保護を目的とする鍵による施錠や、パスワード照合による起動条件を付加する等により当事者以外の使用を排除する対策が知られている。しかし、コンピュータシステムの装置自体の盗難防止に関しては、殆ど対策が採られていない。

【０００３】

【発明が解決しようとする課題】周辺機器の盗難を防止する１つの方法として、周辺機器をある特定のコンピュータシステムにおいてのみ使用可能とすることが考えられる。しかし、周辺機器には、コンピュータシステム本体に備わっているようなデータ保護機能を設けることが一般的には出来ないので、このような対策を採ることは困難である。

【０００４】本発明は、上記に鑑み、コンピュータシステムの周辺機器の盗難を防止することが出来るコンピュータシステムを提供することを目的とする。

【０００５】

【課題を解決するための手段】本発明のコンピュータシステムは、コンピュータ本体と、該コンピュータ本体に

2

接続される少なくとも１つの周辺機器とを備えるコンピュータシステムにおいて、コンピュータ本体及び周辺機器に夫々識別番号を登録する不揮発性メモリを設け、前記コンピュータ本体が、該コンピュータ本体の不揮発性メモリに登録された識別番号と周辺機器の不揮発性メモリに登録された識別番号とを比較する識別番号比較部と、該識別番号比較部の比較結果に基づいて周辺機器の使用を許可又は不許可とする周辺機器使用判定部とを備えることを特徴とする。

【０００６】本発明のコンピュータシステムの好ましい態様では、上記周辺機器使用判定部が、周辺機器の不揮発性メモリに識別番号を登録する記録機能を更に有する。これにより、例えば、コンピュータ本体と全く同じ識別番号又は関連する識別番号を周辺機器に登録することが出来る。

【０００７】また、上記識別番号比較部が、オペレータによって入力された識別番号と、前記コンピュータ本体の不揮発性メモリに登録された識別番号とを比較する機能を更に有することも好ましい態様である。この場合、コンピュー本体のセキュリティも向上する。

【０００８】本発明のコンピュータシステムでは、周辺機器の使用に先立って、コンピュータ本体の不揮発性メモリに登録された識別番号と周辺機器の不揮発性メモリに登録された識別番号とを識別番号比較部で比較し、その比較結果に基づいて周辺機器使用判定部において周辺機器の使用を許可し又は不許可とするため、事前に登録された周辺機器のみが使用可能となる。かかるコンピュータシステムが設備されるコンピュータシステムの大半を占めるようになれば、盗品の周辺機器の使用は排除される。

【０００９】

【発明の実施の形態】本発明の実施形態例に基づいて本発明を更に詳細に説明する。図１は、本発明の一実施形態例のコンピュータシステムを示す模式的ブロック図である。コンピュータシステムは、コンピュータ本体１０と、複数の（図面上で２つの）周辺機器２０、３０とから構成される。コンピュータ本体１０は、通常のデータ処理を行うデータ処理部１１と、コンピュータ本体の識別番号（ＩＤ）を登録するための不揮発性メモリ１２と、コンピュータ本体１０のＩＤと周辺機器２０、３０のＩＤとを比較するＩＤ比較部１３と、ＩＤ比較部１３の比較結果に従って周辺機器の使用の許可又は不許可を判定する機能を有する周辺機器接続情報記録部１４とを有する。双方の周辺機器２０、３０には、夫々、ＩＤを登録するための不揮発性メモリが設けられている。コンピュータ本体及び周辺機器の不揮発性メモリには、例えばフラッシュＲＯＭが使用できる。

【００１０】図１に示したように、コンピュータ本体１０の不揮発性メモリ１２には、コンピュータ本体の識別記号、”ＡＡＡ”が記録されている。双方の周辺機器２

０、３０にも夫々その識別記号（ＩＤ）が不揮発性メモリに登録されており、入力装置を成す一方の周辺機器２０には識別記号”ＡＡＡ”が、マウスとして構成される他方の周辺機器３０には識別記号”ＢＢＢ”が夫々記録されている。ここで、コンピュータ本体１０の識別記号”ＡＡＡ”と、マウス３０の識別記号”ＢＢＢ”とが異なるので、マウス３０は、コンピュータ本体１０のＩＤ比較部１３からの情報に基づいて、周辺機器接続情報記録部１４によって本コンピュータシステムから排除される。

【００１１】図２は、上記実施形態例のコンピュータシステムにおける処理を示すフロー図である。コンピュータシステムが起動されると（ステップＳ１）、コンピュータ本体のＩＤが登録されているか否かがチェックされる（ステップＳ２）。コンピュータ本体のＩＤが不揮発性メモリ内に登録されていなければ、ＩＤ登録のキー入力が前後２回促され、この２回入力されたＩＤが相互に同じであることが確認される（ステップＳ３、Ｓ４）。確認されたＩＤをコンピュータ本体のＩＤとしてコンピュータ本体の不揮発性メモリに登録した後に（ステップＳ５）、ステップＳ８に進んでコンピュータ本体の不揮発性メモリをマスクする。このマスクにより、再び電源が投入されるまでは少なくともＩＤのリード／ライトを禁止する。

【００１２】ステップＳ２でコンピュー本体のＩＤの登録済が確認されると、オペレータに対してＩＤ照合のためのキー入力が促される。ＩＤのキー入力があると（ステップＳ６）、コンピュータ本体の不揮発性メモリに登録されたＩＤと、キー入力されたＩＤとが照合される（ステップＳ７）。照合の結果、双方のＩＤが不一致であると、ステップＳ６に戻り再度のＩＤ入力が促される。双方のＩＤが一致すれば、ステップＳ８の不揮発性メモリのマスクに移る。

【００１３】ステップＳ８に引き続き、周辺機器の接続の有無がチェックされ（ステップＳ９）、接続が確認された周辺機器の１つについて、そのＩＤが登録されているか否かがチェックされる（ステップＳ１０）。ＩＤが未登録であれば、周辺機器接続情報記録部は、周辺機器の不揮発性メモリに、コンピュータ本体のＩＤと同じＩＤを登録する（ステップＳ１１）。その後、通常の処理に従って周辺機器の使用に必要なセットアップを行い（ステップＳ１２）、周辺機器接続情報記録部に当該周辺機器の接続許可を登録し（ステップＳ１３）、ステップＳ１８に移る。

【００１４】ステップＳ１０で、周辺機器のＩＤが既に登録されていれば、そのＩＤがコンピュータ本体のＩＤと同じであるか否かがチェックされる（ステップＳ１４）。周辺機器のＩＤとコンピュータ本体のＩＤとが一致しなければ、その周辺機器の使用を不許可にし（ステップＳ１５）、周辺機器接続情報記録部に当該周辺機器の接続が不許可である旨を登録し（ステップＳ１６）、次いで、ステップＳ１８に移る。

【００１５】ステップＳ１４で双方のＩＤが一致すれば、周辺機器接続情報記録部に、当該周辺機器の接続許可の旨を登録し（ステップＳ１７）、その周辺機器の不揮発性メモリをマスクすることにより（ステップＳ１８）、少なくとも再度電源が投入されるまではその後のリード及びライトを禁止し、当該周辺機器の処理を終了する。その他に周辺機器があれば（ステップＳ１９）、ステップＳ９に戻り、その周辺機器について前述の処理と同様の処理が行われ、その他に周辺機器がなければ、周辺機器についての処理を全て終了する。その後、コンピュータシステムはブート処理に移る（ステップＳ２０）。

【００１６】上記実施形態例では、本コンピュータシステムで使用できる周辺機器２０（図１）、及び、使用できない周辺機器３０についての情報は、コンピュータ本体１０内部の周辺機器接続情報記録部１４に登録してあるので、いつでも参照可能である。

【００１７】なお、上記実施形態例では、不揮発性メモリのマスクにより、再度電源が投入される迄のリード及びライトを禁止した例を示したが、これに代えて、不揮発性メモリにおけるＩＤの登録後は、いかなる書換えをも禁止することも出来る。この場合、セキュリティは更に向上する。

【００１８】また、周辺機器接続情報記録部によって、周辺機器の使用の許可又は不許可を判定する例を挙げたが、これに代えて、周辺機器使用判定部を別のプログラムとして設けてもよい。また、照合のためにコンピュータ本体のＩＤをキー入力して、これと登録されたＩＤとを照合する例を挙げたが、これに加えて、オペレータ自身のＩＤを入力して照合するようにしてもよい。

【００１９】以上、本発明をその好適な実施形態例に基づいて説明したが、本発明は、上記実施形態例の構成にのみ限定されるものではなく、上記実施形態例の構成から種々の修正及び変更を施したコンピュータシステムも、本発明の範囲に含まれる。

【００２０】

【発明の効果】以上、説明したように、本発明のコンピュータシステムによると、コンピュータ本体及び周辺機器の双方のＩＤを比較照合した結果に基づいて周辺機器の使用を許可するように構成したので、コンピュータシステムの周辺機器の盗難を抑止する効果がある。

【図面の簡単な説明】

【図１】本発明の一実施形態例のコンピュータシステムの模式的ブロック図。

【図２】図１の実施形態例のコンピュータシステムにおける処理を示すフローチャート。

【符号の説明】

１０　コンピュータ本体

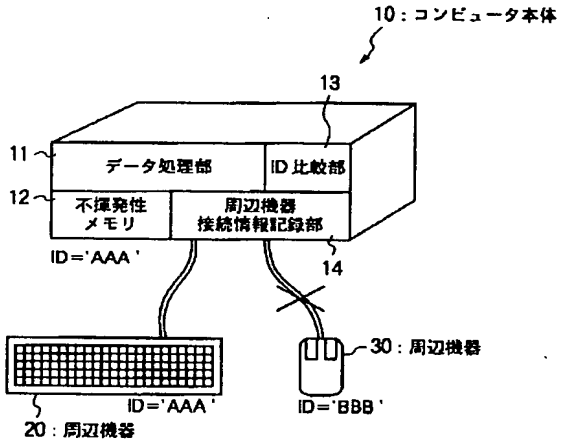
5

１１　データ処理部
１２　不揮発性メモリ
１３　周辺機器接続情報記録部

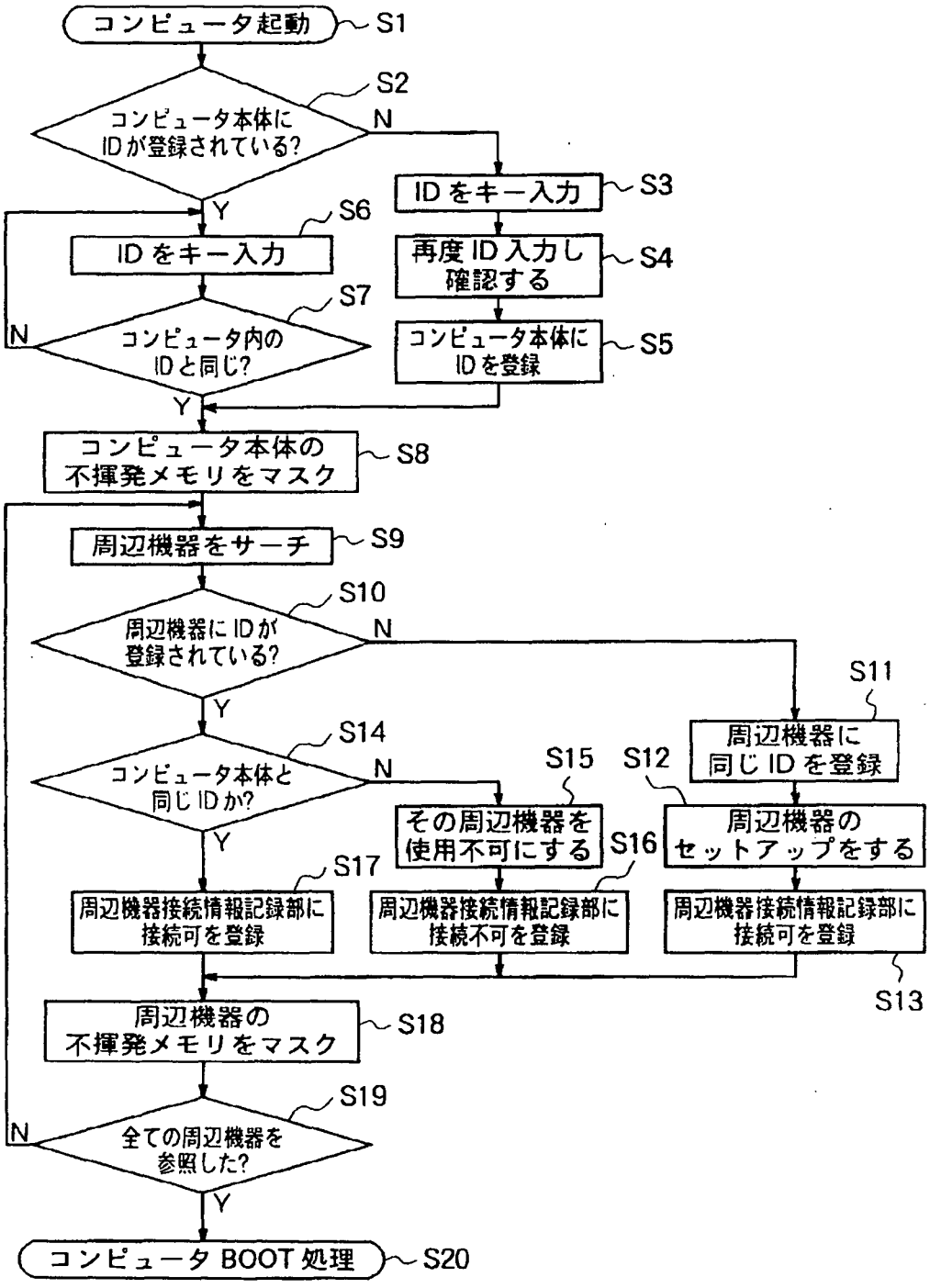
6

１４　ＩＤ比較部
２０　周辺機器（入力装置）
３０　周辺機器（マウス）

【図１】



【図２】


コンピュータ起動
S1
コンピュータ本体に IDが登録されている?
S2
N
Y
IDをキー入力
S3
再度ID入力し 確認する
S4
コンピュータ本体に IDを登録
S5
IDをキー入力
S6
コンピュータ内の IDと同じ?
S7
N
Y
コンピュータ本体の 不揮発メモリをマスク
S8
周辺機器をサーチ
S9
周辺機器にIDが 登録されている?
S10
N
Y
周辺機器に 同じIDを登録
S11
S12
コンピュータ本体と 同じIDか?
S14
N
Y
その周辺機器を 使用不可にする
S15
S16
周辺機器のセットアップをする
周辺機器接続情報記録部に 接続可を登録
S17
周辺機器接続情報記録部に 接続不可を登録
周辺機器接続情報記録部に 接続可を登録
S13
周辺機器の 不揮発メモリをマスク
S18
全ての周辺機器を 参照した?
S19
N
Y
コンピュータ BOOT処理
S20